

130.22.06

ANEXO No. 6 – PROTOCOLO DE SEGURIDAD TECNOLÓGICA Y PLAN DE CONTINGENCIA PARA LA CONTINUIDAD OPERATIVA DEL DATACENTER DURANTE LA INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DEL SISTEMA SOLAR FOTOVOLTAICO (SSFV).

OBJETO: ADQUISICION, INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN SISTEMA SOLAR FOTOVOLTAICO (OFF-GRID Y ON-GRID) PARA LA CONTRALORÍA DEPARTAMENTAL DE CASANARE.

ENTIDAD: CONTRALORÍA DEPARTAMENTAL DE CASANARE.

ÁREA DE INTERVENCIÓN: Datacenter e infraestructura tecnológica institucional.

RESPONSABLE DE APLICACIÓN Y CUMPLIMIENTO DEL PROTOCOLO: Contratista SISTEMA SOLAR FOTOVOLTAICO (OFF-GRID Y ON-GRID).

RESPONSABLE SEGUIMIENTO Y VIABILIDAD AL CUMPLIMIENTO DEL PROTOCOLO: Profesional de Sistemas de la Contraloría Departamental de Casanare.

1. INTRODUCCIÓN

La Contraloría Departamental de Casanare requiere implementar un sistema solar fotovoltaico (SSFV), con componentes de operación ON-GRID y OFF-GRID, con el propósito de mejorar la disponibilidad del suministro energético y contribuir a la continuidad de los servicios tecnológicos institucionales.

La ejecución de las actividades de instalación, conexión, configuración, pruebas y puesta en funcionamiento del sistema fotovoltaico puede implicar maniobras eléctricas, interrupciones programadas, variaciones en el suministro de energía o fallas durante la transición entre la red comercial y el nuevo sistema de generación y respaldo.

Estas situaciones pueden afectar el funcionamiento de los servidores, los sistemas de almacenamiento, las bases de datos, los dispositivos de comunicaciones y las aplicaciones que soportan los procesos administrativos y misionales de la entidad.

Por lo anterior, se establece el presente **PROTOCOLO DE SEGURIDAD TECNOLÓGICA Y PLAN DE CONTINGENCIA**, cuyo propósito es definir las actividades que deberá garantizar el contratista antes, durante y después de las intervenciones eléctricas, así como las acciones que deberá coordinar cuando se presenten fallas que puedan comprometer la disponibilidad, integridad o recuperación de la información institucional.

El protocolo contempla los servicios tecnológicos actualmente identificados en el datacenter de la Contraloría Departamental de Casanare y establece procedimientos para prevenir incidentes, detectar oportunamente las fallas, activar medidas de contingencia y verificar la recuperación de los servicios.

2. OBJETIVO GENERAL

Establecer las medidas preventivas, los procedimientos de actuación y las acciones de recuperación que deberá garantizar el contratista para proteger la infraestructura tecnológica del datacenter y mantener, en la medida de las condiciones técnicas disponibles, la continuidad de los servicios informáticos institucionales durante la instalación y puesta en funcionamiento del sistema solar fotovoltaico.

3. OBJETIVOS ESPECÍFICOS

1. Identificar los riesgos tecnológicos derivados de las interrupciones, las variaciones del suministro eléctrico y las maniobras de transición entre la red comercial y el sistema solar fotovoltaico.
2. Establecer las actividades de verificación previas al inicio de las intervenciones eléctricas.
3. Definir las funciones del ingeniero de sistemas durante las pruebas y los cambios de alimentación eléctrica.
4. Establecer acciones de contingencia frente a la caída de servidores, fallas de almacenamiento, indisponibilidad de aplicaciones y pérdida de conectividad.
5. Definir el procedimiento para recuperar y validar los servicios tecnológicos afectados.
6. Establecer mecanismos de registro, documentación y reporte de incidentes para garantizar la trazabilidad de las actuaciones.
7. Determinar las condiciones mínimas para autorizar la continuidad de las pruebas y la recepción tecnológica de los servicios una vez finalizadas las intervenciones.

4. ALCANCE

El presente protocolo aplica a las actividades relacionadas con la instalación, conexión, configuración, pruebas y puesta en funcionamiento del sistema solar fotovoltaico que puedan afectar directa o indirectamente la infraestructura tecnológica del datacenter de la Contraloría Departamental de Casanare.

Comprende las actuaciones que deberá garantizar el contratista antes, durante y después de las maniobras eléctricas, incluyendo la coordinación con el contratista responsable del SSFV, el supervisor del contrato y el personal técnico de la entidad.

El protocolo cubre los siguientes sistemas y servicios tecnológicos:

1. SIGD – Ventanilla Única.
2. Sistema Contable y Financiero SYSMAN.
3. Sistema de backup compuesto por tres (3) nodos de servidores y dos (2) dispositivos NAS.
4. Sistema de biometría y control de acceso BIOSTAR.
5. Sistema de soporte y mesa de ayuda GLPI.
6. Sistema de videovigilancia CCTV.
7. Sistema de administración de antivirus KASPERSKY.

También comprende los servidores físicos o virtuales, los sistemas operativos, las bases de datos, las redes de comunicaciones, los dispositivos de almacenamiento, CCTV y los componentes de infraestructura tecnológica necesarios para el funcionamiento de los servicios mencionados.

Las actividades de intervención eléctrica, maniobra de tableros, conexión de circuitos, operación de inversores, manipulación de baterías y modificación de protecciones eléctricas serán responsabilidad del contratista y del personal que este disponga previa autorización de la supervisión.

5. SISTEMAS TECNOLÓGICOS OBJETO DE PROTECCIÓN

SISTEMA O SERVICIO	FUNCIÓN INSTITUCIONAL	RIESGO ANTE INTERRUPCIONES ELÉCTRICAS	ACTIVIDADES DEL INGENIERO DE SISTEMAS
SIGD – Ventanilla Única	Gestión documental y atención de trámites y comunicaciones institucionales.	Indisponibilidad de la aplicación, interrupción de transacciones o afectación de la información en proceso.	Verificar disponibilidad, acceso, funcionamiento de la aplicación y consistencia de la información después de las pruebas.
SYSMAN – Sistema Contable y Financiero	Soporte a los procesos contables y financieros.	interrupción de operaciones, pérdida de conexión con la base de datos o errores derivados de un apagado inesperado.	Coordinar la protección de la aplicación y sus bases de datos; validar el acceso y las operaciones autorizadas después de la recuperación.
Sistema de backup: tres nodos y dos NAS	Respaldo y recuperación de información institucional.	Interrupción de tareas de respaldo, indisponibilidad de repositorios o afectación de la capacidad de recuperación.	Verificar el estado de los nodos y NAS, revisar las tareas de respaldo y confirmar que los repositorios sean accesibles.
BIOSTAR	Biometría y control de acceso.	Indisponibilidad del registro biométrico, de la administración del sistema o de sus comunicaciones.	Verificar la disponibilidad de la plataforma y coordinar medidas temporales de control

			de acceso con el personal autorizado.
GLPI	Gestión de incidentes, solicitudes y soporte técnico.	Interrupción del registro y seguimiento de solicitudes de soporte.	Verificar el funcionamiento de la aplicación y asegurar el registro posterior de los incidentes ocurridos durante la intervención.
CCTV	Videovigilancia institucional.	Pérdida temporal de visualización, grabación o acceso a las cámaras.	Verificar cámaras, grabadores, almacenamiento y visualización; informar cualquier pérdida de grabación identificada.
KASPERSKY	Administración y protección antivirus de los equipos y servidores cubiertos.	Interrupción de la comunicación con la consola, pérdida de actualización o disminución de la visibilidad sobre los equipos protegidos.	Verificar la disponibilidad de la consola, la comunicación con los equipos administrados y el estado de protección reportado.

Nota técnica: las verificaciones deberán ajustarse a la arquitectura real de cada sistema, sus dependencias, sus configuraciones y los procedimientos de administración vigentes. No se presume que todos los servicios estén instalados en un mismo servidor ni que compartan una única base de datos.

6. RESPONSABILIDADES

El contratista deberá disponer de personal idóneo que garantice:

1. Conocer la infraestructura tecnológica que pueda verse afectada por la intervención.
2. Identificar los servidores, dispositivos de almacenamiento, equipos de comunicaciones y servicios críticos involucrados.
3. Verificar el estado inicial de los sistemas antes de las maniobras eléctricas.
4. Coordinar con el contratista eléctrico las ventanas de intervención y las pruebas que puedan afectar el suministro energético.
5. Verificar la existencia, vigencia y disponibilidad de los respaldos requeridos para la recuperación de la información.
6. Establecer el orden de apagado y encendido de los equipos cuando técnicamente resulte necesario.
7. Monitorear los servicios tecnológicos durante las pruebas y reportar oportunamente cualquier anomalía.
8. Recomendar la suspensión de las pruebas cuando identifique riesgos relevantes para los servidores, la información o los servicios institucionales.

9. Ejecutar o coordinar, dentro de sus competencias y autorizaciones, las acciones de diagnóstico y recuperación tecnológica.
10. Verificar la disponibilidad de las aplicaciones después de cada intervención.
11. Registrar los incidentes, las decisiones adoptadas, las pruebas realizadas y los resultados obtenidos.
12. Informar al supervisor del contrato y al responsable tecnológico de la entidad sobre cualquier incidente que afecte la continuidad de los servicios.

7. PROCEDIMIENTO PREVENTIVO ANTES DE INICIAR LAS PRUEBAS ELÉCTRICAS

Ninguna prueba que implique una posible interrupción del suministro al datacenter deberá comenzar sin que se hayan coordinado las actividades de protección tecnológica y las maniobras eléctricas previstas.

Inventario y diagnóstico inicial

El contratista con personal idóneo deberá realizar un reconocimiento de la infraestructura tecnológica y elaborar o actualizar un inventario que contenga, como mínimo:

- Identificación de los servidores físicos y virtuales involucrados.
- Identificación de los tres nodos de servidores y los dos NAS del sistema de backup.
- Sistemas operativos y servicios que se ejecutan en los equipos.
- Aplicaciones y servicios institucionales que dependen de la infraestructura.
- Dispositivos de red y comunicaciones necesarios para acceder a las aplicaciones.
- Dependencias entre aplicaciones, servidores, bases de datos y almacenamiento.
- Ubicación de los equipos y circuitos de alimentación, con base en la información validada con el personal eléctrico.
- Responsables técnicos y medios de contacto para atender incidentes.

El inventario deberá permitir determinar qué servicios podrían quedar afectados ante una pérdida de energía y qué dependencias deben restablecerse primero.

Verificación del estado de los sistemas

Antes de las maniobras, el contratista con su personal idóneo deberá comprobar y registrar el estado operativo de los servicios relacionados en el numeral 5.

La verificación deberá incluir:

- a. Acceso a las aplicaciones institucionales.
- b. Estado de los servidores y servicios necesarios para su funcionamiento.
- c. Conectividad de red y disponibilidad de los dispositivos de comunicaciones.
- d. Estado de los tres nodos de backup y los dos NAS.
- e. Estado de las tareas de respaldo y de los últimos resultados registrados.
- f. Funcionamiento del sistema de control de acceso BIOSTAR.
- g. Disponibilidad de la visualización y grabación del CCTV.

- h. Estado de comunicación de los equipos administrados por KASPERSKY.
- i. Disponibilidad de GLPI y de los mecanismos alternativos para registrar incidentes.
- j. Identificación de errores, alertas o fallas preexistentes que puedan confundirse con afectaciones derivadas de las pruebas.

Las anomalías encontradas deberán documentarse y comunicarse antes de iniciar las actividades eléctricas.

Verificación de respaldos y recuperación

El contratista con su personal idóneo deberá revisar que existan respaldos recientes de la información crítica, conforme a las políticas institucionales, y comprobar que los repositorios de respaldo se encuentren accesibles.

Adicionalmente, deberá:

1. Revisar los registros de ejecución de las tareas de backup.
2. Confirmar que los respaldos requeridos hayan finalizado satisfactoriamente o documentar las limitaciones identificadas.
3. Verificar que se disponga de los medios, accesos y procedimientos necesarios para ejecutar una recuperación.
4. Identificar las configuraciones y dependencias necesarias para restablecer los servicios.
5. Confirmar que los mecanismos de recuperación sean viables antes de autorizar una intervención que represente un riesgo significativo.

Cuando se requiera una prueba de restauración, esta deberá realizarse de manera controlada y autorizada, evitando modificar o sobrescribir la información de producción.

Coordinación de la ventana de intervención

Antes de cada maniobra, el contratista con su personal idóneo deberá participar en una reunión o coordinación técnica con el contratista eléctrico y el responsable designado por la entidad.

En dicha coordinación se deberán definir:

- Fecha y hora de inicio y finalización previstas.
- Circuitos y equipos que serán intervenidos.
- Fuente de alimentación que se utilizará durante cada etapa.
- Secuencia de transición entre la red comercial y el SSFV.
- Posibles interrupciones del suministro.
- Servicios tecnológicos que podrían verse afectados.
- Necesidad de apagado controlado de equipos, cuando corresponda.
- Procedimiento de contingencia y condiciones para suspender las pruebas.
- Responsables de ejecutar cada actividad.
- Criterios para declarar estable el suministro y reanudar los servicios.

El contratista con su personal idóneo deberá recomendar que las pruebas con mayor riesgo se programen en una ventana de mantenimiento previamente acordada, considerando los horarios de operación y la criticidad de los servicios.

Definición del orden de apagado y encendido

Cuando las pruebas requieran apagar equipos, la secuencia deberá definirse con base en la arquitectura real del datacenter, las instrucciones de los fabricantes y las dependencias entre servicios.

El ingeniero deberá preparar y documentar el procedimiento aplicable, sin asumir que todos los equipos pueden apagarse o encenderse simultáneamente.

No se deberán apagar de forma abrupta los servidores, las bases de datos, los nodos de respaldo o los dispositivos de almacenamiento mientras exista una alternativa segura de apagado controlado.

Si no se conoce con certeza la secuencia adecuada para un equipo o servicio, deberá solicitarse la validación del administrador responsable o del fabricante antes de ejecutar la maniobra.

Condiciones para autorizar el inicio

Antes de iniciar la transición eléctrica, el contratista con su personal idoneo deberá dejar constancia de que:

- Se realizó la verificación del estado inicial de los servicios.
- Se revisó el estado de los respaldos.
- Se identificaron las dependencias tecnológicas críticas.
- Se acordó el procedimiento de intervención con el contratista eléctrico.
- Se encuentran definidos los responsables y los medios de comunicación.
- Se establecieron las condiciones para detener las pruebas y recuperar los servicios.

Si se identifica un riesgo no controlado, una falla previa relevante, ausencia de respaldos indispensables o falta de claridad sobre la secuencia de intervención, el contratista con su personal idóneo deberá recomendar la suspensión del inicio hasta que se adopten las medidas correspondientes.

8. PROCEDIMIENTO DURANTE LA INSTALACIÓN Y LA TRANSICIÓN ELÉCTRICA

Durante las actividades de instalación, conexión y puesta en funcionamiento del SSFV, el contratista con su personal idóneo deberá permanecer disponible y realizar seguimiento a los servicios tecnológicos afectados por las pruebas.

Monitoreo durante la transición

Durante cada cambio de fuente de alimentación, deberá:

1. Mantener comunicación con el responsable de la maniobra eléctrica.
2. Registrar la hora de inicio y finalización de cada etapa relevante.
3. Monitorear el estado de los servidores y servicios críticos.
4. Verificar la conectividad de los equipos y la disponibilidad de las aplicaciones.
5. Observar alertas de los sistemas de almacenamiento y backup.
6. Confirmar la disponibilidad de los mecanismos de administración y monitoreo.
7. Reportar inmediatamente cualquier apagado inesperado, reinicio, pérdida de conectividad, error de almacenamiento o indisponibilidad de los servicios.
8. Evitar que se reanuden las pruebas mientras persistan fallas tecnológicas sin evaluar.

Actuación ante variaciones o interrupciones del suministro

Si se presenta una interrupción, transferencia fallida, reinicio inesperado de equipos o cualquier comportamiento anormal, el contratista con su personal idóneo deberá:

1. Informar inmediatamente al contratista eléctrico y al supervisor o responsable de la entidad.
2. Solicitar la suspensión de la siguiente maniobra hasta evaluar el incidente.
3. Determinar qué equipos y servicios fueron afectados.
4. Registrar los síntomas observados y la hora aproximada de inicio.
5. Solicitar al personal eléctrico autorizado que verifique la condición del suministro y de los componentes eléctricos.
6. Evitar reinicios repetidos, encendidos forzados o intervenciones que puedan agravar el daño.
7. Aplicar el procedimiento de contingencia correspondiente.
8. Mantener informados a los responsables de la entidad sobre el estado de los servicios.

9. PLAN DE CONTINGENCIA ANTE INCIDENTES

El siguiente procedimiento se aplicará cuando una falla durante la intervención eléctrica comprometa la disponibilidad de los servicios tecnológicos.

Fase 1. Detección y comunicación

Al detectar una falla, el contratista con su personal idóneo deberá:

- Identificar el servicio afectado.
- Registrar la hora y las condiciones en que ocurrió el incidente.
- Informar al contratista eléctrico y al supervisor del contrato.
- Determinar preliminarmente si la afectación es general o se limita a un equipo o aplicación.
- Solicitar que se suspendan temporalmente las pruebas que puedan agravar la situación.
- Establecer un medio de comunicación alternativo si GLPI, la red o los servicios de correo institucional no están disponibles.

Fase 2. Protección de la infraestructura

Una vez detectada la falla, el contratista con su personal idóneo deberá priorizar la protección de los equipos y de la información.

Para ello deberá:

1. Coordinar la evaluación de la estabilidad del suministro con el contratista eléctrico.
2. Verificar el estado de alimentación reportado para los equipos críticos.
3. Evitar el encendido de servidores y dispositivos mientras no existan condiciones eléctricas estables y seguras.
4. Determinar si procede un apagado controlado de los equipos que continúen operando y estén expuestos a un riesgo inminente, siempre que sea técnicamente seguro.
5. Evitar la manipulación de sistemas de almacenamiento o bases de datos sin un procedimiento de recuperación definido.
6. Preservar los registros y evidencias que permitan identificar la causa del incidente.

Si se presenta olor a quemado, humo, temperatura anormal, ruido inusual o cualquier señal de peligro eléctrico, deberá priorizarse la seguridad de las personas, evitar la manipulación de los equipos y solicitar la intervención inmediata del personal competente.

Fase 3. Diagnóstico tecnológico

Una vez controlada la condición eléctrica, el contratista con su personal idóneo deberá verificar:

- Estado de encendido de servidores y dispositivos.
- Disponibilidad de los sistemas operativos y servicios requeridos.
- Estado de las interfaces y conexiones de red.
- Acceso a los volúmenes y repositorios de almacenamiento.
- Estado de los tres nodos de backup y los dos NAS.
- Alertas de integridad de discos, sistemas de archivos o bases de datos.
- Disponibilidad de las aplicaciones institucionales.
- Registros de errores y eventos producidos durante la interrupción.

El diagnóstico deberá permitir establecer si la falla corresponde a una interrupción de alimentación, un problema de red, una indisponibilidad de un servidor, un error de almacenamiento, una falla de aplicación o una combinación de estos factores.

Fase 4. Recuperación de los servicios

La recuperación deberá realizarse en un orden previamente documentado, sujeto a la arquitectura tecnológica real y a las instrucciones de los administradores responsables.

Como orientación general, se deberá considerar la siguiente secuencia:

1. **Estabilización eléctrica:** el contratista eléctrico confirma que la alimentación se encuentra en condiciones seguras y estables.

2. **Infraestructura base:** verificar la disponibilidad de los equipos de red, conectividad y demás componentes requeridos por los servidores.
3. **Servidores y almacenamiento:** iniciar o recuperar los equipos según las dependencias identificadas y las instrucciones técnicas aplicables.
4. **Servicios de soporte:** verificar los servicios de autenticación, bases de datos, almacenamiento y demás componentes de los que dependan las aplicaciones.
5. **Aplicaciones institucionales:** comprobar el funcionamiento de SIGD, SYSMAN, GLPI, BIOSTAR y los demás servicios.
6. **Sistemas de protección y monitoreo:** verificar CCTV y KASPERSKY, junto con los mecanismos de supervisión disponibles.
7. **Sistema de respaldo:** comprobar el estado de los tres nodos, los dos NAS y las tareas de backup, sin iniciar restauraciones innecesarias.
8. **Validación final:** realizar pruebas funcionales con los responsables de cada servicio y registrar los resultados.

Este orden es orientativo. Si la arquitectura real establece dependencias distintas, el ingeniero deberá aplicar la secuencia documentada para la infraestructura de la entidad.

No se deberá iniciar una restauración de datos, reconstrucción de nodos o recuperación de bases de datos sin identificar previamente el alcance del daño, el respaldo apropiado y los riesgos de sobrescribir información válida.

Fase 5. Validación y cierre del incidente

Una vez recuperados los servicios, el contratista con su personal idóneo deberá:

- Confirmar el acceso a cada aplicación.
- Verificar la disponibilidad de los servicios de base de datos y almacenamiento que correspondan.
- Comprobar que los sistemas de backup estén operativos y que sus tareas puedan ejecutarse.
- Verificar la visualización y grabación del CCTV.
- Comprobar el estado de comunicación de los equipos administrados por KASPERSKY.
- Validar el funcionamiento de BIOSTAR con el responsable institucional.
- Confirmar el funcionamiento de SIGD, SYSMAN y GLPI con los usuarios autorizados.
- Registrar las fallas persistentes y las limitaciones que no hayan podido resolverse.
- Informar al supervisor sobre el resultado de la recuperación.

La reanudación de las pruebas eléctricas deberá contar con la coordinación y autorización correspondiente, una vez identificada la causa del incidente y verificadas las condiciones necesarias para continuar de manera segura.

10. PROCEDIMIENTOS ESPECÍFICOS POR SISTEMA

SIGD – Ventanilla Única

Ante una interrupción o indisponibilidad del SIGD, el contratista con su personal idóneo deberá:

1. Verificar la conectividad con el servidor y los servicios de los que depende la aplicación.
2. Comprobar el estado de la aplicación y de su base de datos, cuando corresponda.
3. Revisar los registros de eventos disponibles.
4. Confirmar si existen transacciones interrumpidas o procesos pendientes.
5. Coordinar con el administrador del sistema las acciones necesarias para recuperar el servicio.
6. Solicitar al responsable funcional que valide el acceso y el procesamiento normal de las operaciones.
7. Informar a la dependencia usuaria si se requiere activar un procedimiento manual temporal para la recepción o gestión de documentos.

No deberán repetirse operaciones ni modificarse registros sin verificar previamente si la transacción original se completó.

SYSMAN – Sistema Contable y Financiero

Ante una interrupción del sistema contable y financiero, el contratista con su personal idóneo deberá:

1. Verificar el estado del servidor de aplicación y de la base de datos correspondiente.
2. Revisar los registros de error para determinar si hubo una interrupción durante operaciones de escritura.
3. Confirmar la disponibilidad y consistencia de la base de datos con el administrador responsable.
4. Evitar restauraciones o modificaciones directas de datos sin autorización y evaluación técnica.
5. Coordinar las acciones de recuperación con el administrador del sistema y el responsable funcional.
6. Solicitar pruebas de acceso y de consulta, así como otras operaciones de validación autorizadas.
7. Registrar cualquier transacción que requiera revisión por parte del área financiera.

La validación funcional de la información contable deberá contar con el apoyo del personal autorizado del área financiera.

Sistema de backup: tres nodos y dos NAS

Este componente deberá recibir especial atención debido a su importancia para la recuperación de la información institucional.

Ante una falla, el contratista con su personal idóneo deberá:

1. Verificar el estado individual de los tres nodos de servidores.
2. Comprobar la disponibilidad de los dos NAS y la conectividad con los repositorios de respaldo.
3. Revisar las alertas de almacenamiento, los registros de error y el estado de los trabajos de backup.
4. Identificar si alguna tarea de respaldo quedó interrumpida.
5. Evitar iniciar trabajos masivos de respaldo o restauración mientras no se conozca el estado de los repositorios.

6. Determinar, junto con el administrador responsable, si existe riesgo de pérdida o inconsistencia de información.
7. Verificar que los respaldos previos a la intervención continúen disponibles.
8. Si se requiere restauración, identificar el respaldo apropiado, el alcance de la recuperación y la autorización necesaria.
9. Documentar las tareas fallidas y verificar su ejecución posterior.

La restauración deberá efectuarse de manera controlada y con trazabilidad. No se deberán sobrescribir repositorios ni eliminar copias de respaldo como medida improvisada de recuperación.

BIOSTAR – Biometría y control de acceso

Ante una falla de BIOSTAR, el contratista con su personal idóneo deberá:

1. Verificar la conectividad del servidor o equipo que administra la plataforma.
2. Comprobar la disponibilidad de la aplicación y la comunicación con los dispositivos correspondientes.
3. Revisar el estado de los servicios de administración y de los registros disponibles.
4. Informar al responsable institucional de seguridad o control de acceso.
5. Coordinar un procedimiento temporal de acceso autorizado, si resulta necesario.
6. Verificar el restablecimiento de la plataforma y el registro de los eventos que correspondan.

No deberán deshabilitarse controles de acceso ni implementarse mecanismos que permitan el ingreso sin autorización. Las medidas temporales deberán ser aprobadas por la entidad.

GLPI – Mesa de ayuda

Si GLPI deja de funcionar, el contratista con su personal idóneo deberá:

1. Verificar la disponibilidad de la aplicación, el servidor y la base de datos correspondiente.
2. Revisar los registros de error y la conectividad.
3. Recuperar el servicio conforme al procedimiento técnico aplicable.
4. Mantener un registro alternativo de los incidentes atendidos mientras la herramienta esté fuera de servicio.
5. Tras el restablecimiento, registrar o trasladar a GLPI los incidentes, las acciones ejecutadas y los resultados.

El registro alternativo deberá incluir fecha, hora, servicio afectado, descripción de la falla, responsable y acción adoptada.

CCTV – Videovigilancia

Ante una interrupción del CCTV, el contratista con su personal idóneo deberá:

1. Verificar la disponibilidad de la infraestructura de red y de los equipos de grabación.

2. Comprobar la conectividad de las cámaras y la disponibilidad de la plataforma de visualización.
3. Revisar el estado del almacenamiento y de las grabaciones.
4. Identificar, cuando sea técnicamente posible, el periodo durante el cual pudo haberse interrumpido la grabación.
5. Informar al responsable de seguridad de la entidad.
6. Verificar la recuperación de la visualización y grabación de las cámaras.
7. Documentar las cámaras o periodos de grabación que continúen afectados.

No deberá afirmarse que existe continuidad de las grabaciones sin verificar efectivamente la disponibilidad del material correspondiente.

KASPERSKY – Administración de antivirus

Ante una interrupción del sistema de administración de antivirus, el contratista con su personal idóneo deberá:

1. Verificar la disponibilidad de la consola de administración.
2. Comprobar la comunicación con los equipos y servidores administrados.
3. Revisar las alertas y los registros de eventos disponibles.
4. Confirmar que los equipos continúen contando con los mecanismos de protección que tengan instalados.
5. Restablecer la comunicación con la consola siguiendo el procedimiento autorizado.
6. Verificar el estado reportado de protección y actualización de los equipos.
7. Registrar los dispositivos que no puedan ser administrados o cuya protección no pueda verificarse.

No deberán deshabilitarse los mecanismos de protección antivirus como solución improvisada a una falla de conectividad o disponibilidad.

11. CRITERIOS PARA SUSPENDER O NO REANUDAR LAS PRUEBAS

El contratista con su personal idóneo deberá informar inmediatamente al supervisor y solicitar la suspensión de las pruebas que puedan agravar la situación cuando se presente cualquiera de las siguientes condiciones:

1. Apagado o reinicio inesperado de servidores críticos.
2. Indisponibilidad simultánea de varios servicios institucionales.
3. Pérdida de conectividad con los sistemas de almacenamiento o los repositorios de backup.
4. Errores que puedan comprometer la integridad de las bases de datos.
5. Ausencia de confirmación sobre la estabilidad del suministro eléctrico.
6. Fallas repetidas durante las transferencias entre fuentes de alimentación.
7. Alarmas que indiquen posibles daños en equipos o sistemas de almacenamiento.
8. Falta de disponibilidad de los responsables técnicos necesarios para ejecutar una recuperación segura.
9. Ausencia de condiciones para verificar la integridad y disponibilidad de la información.

10. Cualquier condición que represente un riesgo no controlado para la infraestructura tecnológica o para la seguridad de las personas.

La suspensión se mantendrá hasta que el contratista eléctrico y el personal competente corrijan las condiciones que les correspondan, se evalúe la afectación tecnológica y el supervisor o responsable autorizado permita reanudar las pruebas.

12. REGISTRO Y REPORTE DE INCIDENTES

Todo incidente ocurrido durante las maniobras deberá documentarse, incluso si se resuelve en el mismo momento y no genera una interrupción prolongada.

El registro deberá contener, como mínimo:

- Número consecutivo del incidente.
- Fecha y hora de detección.
- Actividad eléctrica que se estaba ejecutando.
- Descripción de la condición observada.
- Sistemas y equipos afectados.
- Posible causa, diferenciando hechos verificados de hipótesis.
- Acciones preventivas o correctivas ejecutadas.
- Personas o responsables que intervinieron.
- Tiempo de indisponibilidad, cuando pueda determinarse.
- Estado final del servicio.
- Evidencias técnicas disponibles.
- Recomendaciones para evitar la repetición del incidente.
- Aprobación o validación del responsable correspondiente, cuando proceda.

El ingeniero deberá presentar al supervisor un informe de las actividades de acompañamiento tecnológico, las pruebas realizadas, las contingencias presentadas, las acciones ejecutadas y el estado final de los servicios.

13. CONSIDERACIONES FINALES

El presente protocolo constituye un instrumento de prevención, coordinación y respuesta para reducir los riesgos tecnológicos asociados a la instalación y puesta en funcionamiento del sistema solar fotovoltaico de la Contraloría Departamental de Casanare.

Su aplicación requiere la participación coordinada del ingeniero de sistemas de la Contraloría Departamental de Casanare y el contratista eléctrico, el supervisor del contrato y los responsables institucionales de los servicios tecnológicos.

La disponibilidad de respaldos, la verificación previa de los sistemas, la coordinación de las ventanas de mantenimiento y la aplicación de procedimientos de recuperación son medidas esenciales para reducir el riesgo de pérdida de información y de interrupción de los servicios institucionales.

El contratista con su personal idóneo deberá actuar oportunamente frente a las anomalías identificadas, documentar sus actuaciones y solicitar la suspensión de las pruebas cuando las condiciones puedan comprometer la infraestructura tecnológica. Sin embargo, no podrá actuar sin aprobación del profesional de sistemas de la Contraloría Departamental.

La puesta en funcionamiento del sistema solar fotovoltaico no deberá considerarse suficiente, por sí sola, para declarar restablecidos los servicios tecnológicos. La conformidad del componente tecnológico deberá sustentarse en las verificaciones funcionales, las evidencias obtenidas y el registro de las novedades que permanezcan pendientes.

En consecuencia, el cumplimiento de este protocolo contribuirá a que la transición energética se realice de forma coordinada, controlada y documentada, protegiendo la información institucional y procurando la continuidad operativa del DATACENTER durante la ejecución del proyecto.

El presente documento hace parte de las condiciones técnicas del proceso y deberá ser aceptado e incluido en la oferta respectivamente.



DAIMER ALVEIRO PACHECO BAUTISTA

Profesional Universitario
Ingeniero de Sistemas CDC